複数組織全体の対応力に着目した CSIRT 活動項目割当方式の検討

小村誠一 [1,*]　後藤厚宏 [1]

概要：リソース不足などから必要と想定するインシデント対応力を実施できない企業のインシデントにより，同一企業グループに属しCSIRTを有する企業が被害にあう事案が発生している．各社のセキュリティ強化だけでなく企業グループ全体の最低インシデント対応能力の向上が重要である．本研究では企業グループ全体として確保すべき対応力を達成するために，CSIRTを活動項目に分解し，活動項目を各社ごとや複数の企業でまとめて利用するなど，企業グループ内で実施を割り当てる方式を検討整理した．活動項目の割当は設定したインシデント対応力の目標や企業グループの状況と，活動項目自体の時間や取扱情報の制約，集約の難易度などで変化する．我々は因果ループ図を用い，活動項目の割り当てによる稼働量や作業の難易度の変化の関係を定式化し，個々の活動項目が各社ごとの構築運用する場合とある企業に集約して複数社で共通利用する場合の分類を整理した．企業グループの状況に応じて集約可能な活動項目を抽出し運用する組織を抑えることで，企業グループ全体が満たすべきインシデント対応機能をより少ないコストで実現することが可能となる．

キーワード：CSIRT，インシデント対応，システムダイナミクス，因果ループ図，構成モデル

CSIRT activity component method for the response capability of multiple organizations as a whole

Seiichi Komura[1,*]　Atsuhiro Goto[1]

Abstract: The incidents of companies with inadequate security measures become more serious, some companies with CSIRTs belonging to the same group have been affected. It is important not only to strengthen the security of individual companies but also to improve the minimum incident response capability of the entire corporate group. We propose the CSIRT activity component method that enables a corporate group to have a self-defined level of incident response capability by appropriately assigning the decomposed CSIRT activity components. The individual implementation or aggregation of activity components varies depending on the situation of the corporate group, the conditions for fulfilling the requirements, the constraints of information sharing of the activity themselves, and the difficulty of aggregation. We used a causal loop diagram to formulate the relationship between changes in response time and operation workloads due to the assignment of activity components.

Keywords: CSIRT, Incident Response, System Dynamics, Causal loop diagram, component model

1. はじめに（研究の背景）

情報セキュリティインシデント（以降，インシデント）が企業や社会に与える影響が深刻化しており，大企業を中心にインシデントに専門で対応する CSIRT の設置が広がっている．一方でセキュリティ対策にそれなりのリソースを支出できる大企業が中核の企業グループであっても，その中にはリソース確保が行えないなどの理由でセキュリティ対策が充分でない中小規模の企業が存在する場合がある．最近はセキュリティ対応が進んでいる大企業を攻撃する前に，その企業グループの CSIRT を設置していないセキュリティ対策の不十分な企業を攻撃し，その企業経由でターゲットとする大企業の顧客を含む機密情報の入手や，ターゲットの大企業の ICT 環境の情報を摂取し攻撃に利用する事案が発生している．そのため大企業のみのセキュリティを強化するだけでなく，企業グループ全体のセキュリティ強化が重要である．

本研究では，企業グループ全体のセキュリティ強化として，CSIRT を複数の活動項目に分解し，それら分解した活動項目を企業グループの各企業の状況に応じて割り当て，企業グループの各企業が設定されたインシデント対応能力の基準を達成することを目指す方法を検討する．本稿の構成は以下の通りである．

- 第２章では，本稿が取り扱う企業グループのセキュリティ課題と関連研究を分析する．
- 第３章では，CSIRT を活動項目に分解する点と企業グループ全体での割当について提案する．
- 第４章では，因果ループ図を用いた企業グループや各企業の状況と活動項目の割合の関係について議論する．

1 情報セキュリティ大学院大学
Institute of Information Security
* dgs214102@iisec.ac.jp

2. 中小規模組織のインシデント対応の課題と関連研究

「はじめに」でも述べたように最近はセキュリティ対策が不十分な企業を足掛かりとしてターゲットとする大企業を狙うマルウェアや APT が発生している．そのため個々の企業のセキュリティ対策を改善するだけでなく企業グループの全社でインシデント対応能力を改善することが重要である．

一般社団法人　損保保険協会が 2020 年 12 月に公開した“国内企業のサイバーリスク意識・対策実態調査 2020”［1］によると，表 1 に示すとおりサイバーリスク対策を行う専門部署を持つ割合は従業員 1,000 名以上の企業が 22.6%である一方，従業員が 100 名以下の企業では 3.1%である．またセキュリティポリシーや事故対応マニュアルの整備については，従業員 1,000 名以上の企業が 58.1%であるのに対し，従業員 100 名以下の企業は 10.6%であり，中小規模の企業に対し，サイバーリスク対応の中核であるインシデント対応力確保を支援する方法を整備することが重要である．

表 1：従業員数によるサイバーリスク対応の状況
“国内企業のサイバーリスク意識・対策
実態調査 2020”［1］をもとに作成

	1,000 名超	100 以下
サイバーリスク対策専門部署がある	22.6%	3.1%
セキュリティポリシーや事故対応マニュアルを策定	58.1%	10.6%

本研究は，インシデント対応を行う人員やリソースを確保できない企業に対し，同一の企業グループに属する他の企業が有する CSIRT の活動の一部を共通で利用することで，その企業のインシデント対応能力を向上させる方法を提案する．CSIRT を複数の活動項目に分解し，自社で構築運用する活動以外に同一企業グループの他企業が運用している活動項目を共通に利用する．これにより自社で単独に構築運用するよりも安価に信頼性の高い運用が行うために，活動項目が個々に構築・運用か，ある企業に集約して共通利用するかを企業の状況や活動内容を基に分析する手法を定式化する．

2.1 CSIRT を複数の活動項目に分解する事例

CSIRT を複数の活動に分解する事例としては FIRST の CSIRT Services Framework［2］がある．CSIRT Services Framework は世界の CSIRT コミュニティである Forum of Incident Response and Security Teams(FIRST)において，世界の CSIRT 専門家が集まり CSIRT がコンスティチュエンシに提供する業務（サービス）を網羅的に整理したもので，表 2 の 5 つサービスエリア，21 のサービスからなる．

表 2 FIRST CSIRT Services Framework[2]のサービス一覧
※番号・名称は日本語版を使用

5	**情報セキュリティイベントマネジメント**
5.1	監視と検知
5.2	イベント分析
6	**情報セキュリティインシデントマネジメント**
6.1	情報セキュリティインシデント報告の受付
6.2	情報セキュリティインシデントの分析
6.3	アーティファクトとフォレンジック
6.4	緩和と回復
6.5	情報セキュリティインシデントの調整
6.6	危機管理支援
7	**脆弱性管理**
7.1	脆弱性の発見・調査
7.2	脆弱性報告の取得
7.3	脆弱性の分析
7.4	脆弱性の調整
7.5	脆弱性の開示
7.6	脆弱性対応
8	**状況把握**
8.1	データ取得
8.2	分析と統合
8.3	コミュニケーション
9	**知識移転**
9.1	啓発
9.2	トレーニングと教育
9.3	演習
9.4	技術およびポリシーに関するアドバイス

CSIRT Services Framework は CSIRT の現状把握や改善を行うために CSIRT の機能や活動を分解し，分解した項目ごとに評価や必要性，改善を行うことに活用できる．

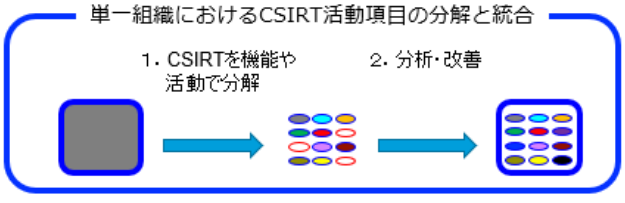

図 1　CSIRT の機能や活動の分解

しかしながら複数の CSIRT で機能や活動を共有することや割り当てることについては触れていない．

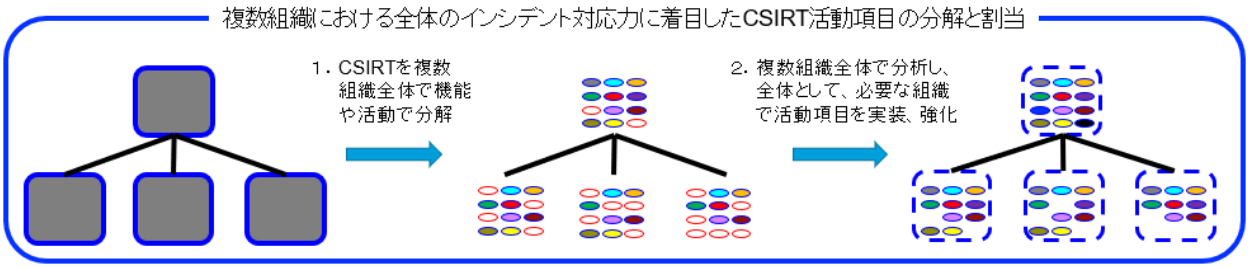

図２　CSIRT を活動項目に分解し，複数の組織に割り当てるイメージ

我々は分解・再構成の対象を単一組織から複数組織に拡張する．CSIRT を活動項目に分解し，活動項目ごとに複数組織内のどの組織に何を割り当てるか，どの組織間で共通で利用するかを決める．そのことにより複数組織全体として，設定したインシデント対応力の目標を達成するために活動項目の状況把握や改善する方法を考案する（図２）．

企業グループ全体での活動項目の割当や共通に利用することにより，インシデント対応を行うためのリソースが確保できない企業は，同一企業グループの他企業が有する CSIRT 活動を活用することで，自前で構築し運用するコストを下げることが可能となる．また同じ活動項目を運用している複数企業でその活動項目を集約し運用することで，企業グループ全体でコストを下げることが可能となる．

2.2 CSIRT 活動の一部を他社に依頼する事例

企業が，他の企業が運用している活動項目を利用する方法としては，企業グループの事例ではなく一般企業がセキュリティ専門会社に業務委託するという事例になるが，ISOG-J が公開している“セキュリティ組織の教科書”[6]の中のモデル ISOMM で議論されている．ISOMM では CSIRT や SOC のようなセキュリティ組織が行う活動に関し，自組織で実施した方がよい活動とセキュリティ専門業者に委託する方がよい活動を以下の２軸を用いて分析している．

- 組織外部の情報 or 攻撃者側の情報
  ↔ 組織内部の情報 or 被害者側の情報
- セキュリティ専門スキルの高 ↔ 低

一つ目の軸は，汎用的な情報か個々の組織固有の情報かという点と誰でも活用可能な情報か限られたメンバのみが閲覧や活用可能な情報かという点である．二つ目の軸は組織の業務と関係のあるスキル（技術や知見，経験など）か組織の業務によらず活用できるスキルかである．

同様に企業グループではなく一般企業がセキュリティ専門会社に業務委託する際の事例になるが，日本シーサート協議会の“CSIRT 人材の定義と確保 v1.5”[7]では，ユーザ企業（IT関連以外の業種）の総務部が実施する CSIRT が，充分な有スキル人員の確保が難しい場合，インシデント対応の判断を行う“コマンダー”は自組織のメンバで行うべきであるが，様々な組織と調整しながらインシデント対応を進める“インシデントハンドラ”は外部に委託することも可能としている．これは一般的なインシデント対応の知見を有している 委託先企業の従業員である“インシデントハンドラ”は状況によっては企業の内部情報を扱うことも可能ということであり，企業の置かれた状況に応じて変化するのである．これは，インシデント対応を含む CSIRT 活動により事業に影響がある場合は自社で対応すべきあるが，それ以外の活動に関しては，状況に応じ外部を使うこともあり得ることを示している．

2.3 一つの組織内で部分 CSIRT を設置する事例

企業ではないが新潟大学の CSIRT では，ネットワークなどを監視する本部 CSIRT と運用しているシステムの状況を把握している部局 CSIRT に分けた体制を敷き活動している［8］．こうすることで，新潟大学内で共通とする基準を基にネットワークの監視・検出や一般的な ICT 技術の知見に基づくインシデント対応・支援を行う本部 CSIRT がインシデントの発生を早期に発見し，業務やシステムの運用状況を把握している部局 CSIRT が業務や運用の状況に応じて対応することで，発災組織の方々と協力しやすい環境を作り，迅速かつ安定的な CSIRT 活動を実現している．

2.4 企業グループ全体のインシデント対応を親会社が行う事例

CSIRT の対象範囲（以降，Constituency）を企業グループ全体とし，親会社の CSIRT で企業グループ内の全企業のインシデント対応を行う事例がある．Constituency を企業グループとすることでリソースと有スキル者を有する企業が，セキュリティ対応が不十分な企業を支援し，インシデントや APT 攻撃の被害軽減や拡大防止を行っている．これにより中小規模の企業はインシデント対応のリソースや人員確保を行う必要はなくなるメリットがあるが，一つの CSIRT で対応するため，全企業の IT システムや運用ルール，セキュリティポリシーを統一することが重要となる．同一の企業グループであっても別企業では業種や業態，企業文化の違いや，独自開発の IT システム構築や運用が異なるため，他企業の CSIRT によるインシデント対応が適

切に行えない場合がある．それを回避するためには，親会社が強力な統治能力を発揮し，システム構成や運用，セキュリティポリシーを統一するとともに，システムやルールの全体最適化を検討・整理しドキュメントへの反映，周知，徹底を行うための稼働と体制の確保が重要とある．

2.5 企業グループ内の複数企業が CSIRT を保有する事例

日本の企業グループに多い事例であるが，企業グループの複数企業が CSIRT を保有し，自社や自社配下のサブグループ企業のインシデント対応を行っている事例がある．企業グループ内の大規模の企業が自社や自社配下のより関係が深い企業を対象にインシデント対応を行うとともに，全体の企業グループ内で情報交換や連携を行い，インシデントの軽減や防止を行うものである．同一企業グループ内でもシステム構成や運用，業態の違いがある場合，一つの CSIRT が全企業グループのインシデント対応を行うよりも，迅速・的確にインシデント対応を行えるというメリットがある．一方，企業グループ全体で集約して実施可能な CSIRT 活動を複数運用している場合がある．要員の配置や活動が最適化されているか把握されていない場合があること，複数の CSIRT のいずれもから対象とされておらずインシデント対応能力が不十分な企業がグループ内に存在する可能性がある懸念がある．

2.6 インシデント対応課題のまとめ

本研究では，企業グループ全体で一定以上のインシデント対応力を保持することを目標として，CSIRT の活動を活動項目に分解し，企業グループの各企業に割り当て，互いに連携し全体としてインシデント対応力を維持向上する方法の構築を目指す．次章以降では，CSIRT が他企業のインシデント関連活動を行う場合に，複数組織で集約することでよりよい結果を得られる CSIRT の活動項目と各社ごとに実施することで不適切な対応を回避しインシデント被害の軽減につながる活動項目など，企業グループ内の活動項目の割当に関する分類を整理する．なお，企業グループに属さない中小規模の企業のインシデント対応力確保の支援は本稿では対象外とする．

3. CSIRT 活動項目割当方式

本稿で提案する“CSIRT 活動項目提案方式”の企業グループへの割当の方法について説明する．

3.1 CSIRT の活動項目の複数組織への割当について

FIRST の CSIRT Services Framework［2］は，CSIRT の活動項目に分解し，自分たちの CSIRT の現時点の状況を把握し，実装や達成すべき目標を決め強化・改善することを示しており，CSIRT の状況把握・改善において有効な方法と言える．しかしながら一つの CSIRT を対象に記述されており，複数企業における全体を俯瞰しての CSIRT 活動の割当や共有については触れていない．本章では，リソース不足などの問題で十分なインシデント対応が行えない企業に対し，同一企業グループ内の複数企業で CSIRT 活動の共有や割り当てを行うことで企業グループ全体において保持すべき対応力を確保すること，全社において一定以上のインシデント対応力を保持する割当の方式を整理する．

3.2 CSIRT の活動項目割当の 4 種類

前節で提起した CSIRT の活動項目について企業グループ内で割当や共同利用を行う方法について述べる．ここで活動項目の割当とは以下の 4 種類とする．

- 実施割当：該当する活動項目を自社で運用するか他社が運用するかに関わらず実施すること
- 個別割当：該当する活動項目を自社のみで要員や体制を整備し自社として運用すること
- 利用割当：該当する活動項目を自社では運用せず，他社が運用するものを利用し，実施すること
- 集約割当：個別割当の一形態で，該当する活動項目を他社も利用できるように運用すること

上記で定義した割当を以下のように行う．

① CSIRT が実施する活動項目を決める．本研究では CSIRT Services Framework の中から選ぶこととする ※表 2 を参照
② 企業の業種や業務内容に応じ，実施する活動項目について個別割当と利用割当を決定する
③ 活動項目で利用割当された企業が存在する場合，有スキル者やリソースの状況に応じ，活動項目ごとに他社も利用できる集約割当を行う企業を決定する

上記割当について，図３の 4 社（A～D）からなる企業グループαを例として説明する．企業グループαは親会社の A とその子会社 B と C，C の子会社 D からなる．設定として，A は小売業を営む企業とする．B は企業グループαのネットワークを運用する A の子会社とする．C は商品を仕入れる A の子会社とする．D は海外の商品を輸入する C の子会社とする．

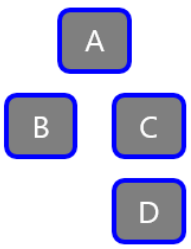

図 3　例として用いる企業グループαの構成

この企業グループにおいて，実施する CSIRT の活動項目について図 4 を用いて説明する．

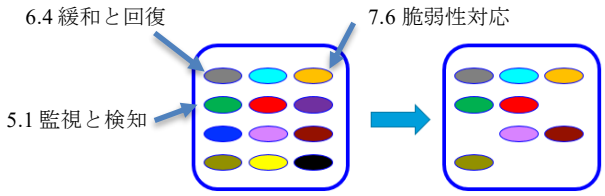

図 4　CSIRT 活動項目の決定

図 4 では，青枠の中の楕円を CSIRT の活動項目とする．左は全項目であり，ここでは例として 12 項目としている．右の青枠の中が企業グループ α で実施することとした活動項目である．これは企業グループ α 全体で何を実施すべきかを決めることである．この後，説明に用いるため，いくつかの活動項目を例示する．図 4 の左側の青枠内の左上の灰色の楕円を FISRT CSIRT Services Framework[2]の“6.情報セキュリティインシデントマネジメント”の“6.4 緩和と回復”とし，左の上から 2 番目の緑色の楕円を“5.情報セキュリティイベントマネジメント”の“5.1 監視と検知”，右上の橙色の楕円を“7. 脆弱性管理”の“7.6 脆弱性対応”とする．企業グループ α ではこれらを含む 8 項目を選んでいる．

次に，各社に対する活動項目の実施割当を決める．企業グループ α としては，図 4 の 8 項目を実施することを決めたが，各社がそれらのうち，なにを行うべきかを決めることである．

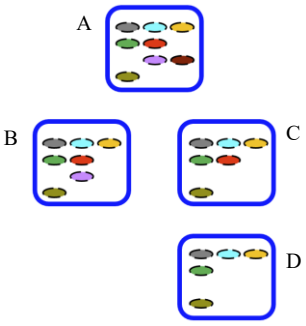

図 5　CSIRT 活動項目の各社への実施割当

図 5 では各社の実施すべき活動項目として選定された実施割当を示している．各社の業務内容や保有する ICT 環境，顧客状況を考慮し，実施すべき CSIRT の活動項目が割り当てられている．すべての企業で，“6.4 緩和と回復”，“5.1 監視と検知”，“7.6 脆弱性対応”を実施割当としている．ただし，各活動項目を自社で体制を構築し運用するかは別であり，別の企業が運用している活動項目を利用するだけの場合も含まれる．

最後に個別割当と利用割当，集約割当を決める．

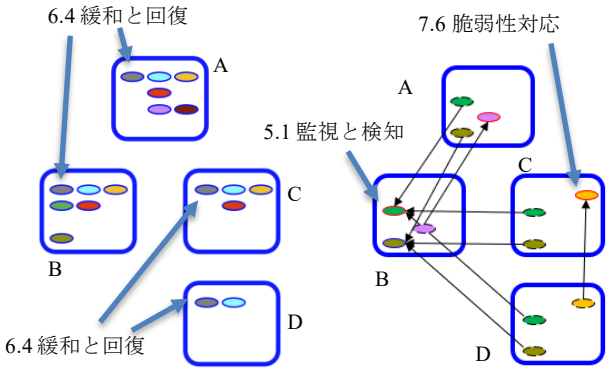

図 6 CSIRT 活動項目の個別割当（左）と
利用割当，集約割当（右）

個別割当は自社の実施割当の中から各社の業務や顧客との契約内容などから自社で要員やリソースを確保し運用するものである．集約割当は自社の個別割当の活動項目を有スキル者やリソースの関係から企業グループの他社が共有し利用できる活動項目である．この例では，“6.4 緩和と回復”は全ての企業が個別割当として実施している．一方“5.1 監視と検知”は企業グループ α のネットワークを運用する企業 B が集約して実施することとして，企業 B には集約割当，企業 A，C，D には利用割当を行っている．また既知の脆弱性対応を行う“7.6 脆弱性対応”については，企業 A，B，C は個別割当としているが，企業 D は利用割当とし，企業 C と D に対して活動する集約割当を企業 C に行っている．上記をまとめると以下の図 7 のようになる．

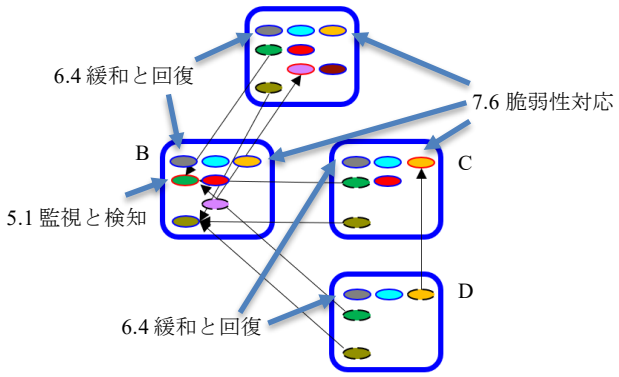

図 7　企業グループ α の CSIRT 活動項目の割当

企業 A は，CSIRT 活動項目の実施割当が 8 項目であり，そのうち，個別割当が 6 項目，集約割当が 1 項目，利用割当が 2 項目，企業 B は実施割当が 7 項目，個別割当が 6 項目，集約割当が 2 項目，利用割当が 1 項目，企業 C は実施割当が 6 項目，個別割当が 4 項目，集約割当が 1 項目，利用割当が 2 項目，企業 D は実施割当が 5 項目，個別割当が 2 項目，集約割当が 0 項目，利用割当が 3 項目である．

4. CSIRT 活動項目割当方式の分析

CSIRT を分解し，活動や Constituency も分解するというやり方を行っている組織は新潟大［8］の例にもあるように存在する．しかしながらどのような機能をどこに割り当てるかについての汎用的な議論は行われていない．本章では企業グループの状況や各活動項目の性質に応じ集約や個別などの割当について考察する．

4.1 CSIRT 活動項目の作業分類

インシデント対応を行う際，発生したインシデントや OS，ミドルウェアなど，個々の企業や部署に関係なく汎用的に必要となる知識と，インシデントが発災した部署の独自開発したシステムや運用の方法，規則，顧客との関係，文化，信頼関係などの個々の組織に関連する知識や関係性が左右する．

CSIRT の活動は汎用的な ICT 技術や世界各地で発生している不正アクセスや APT などの知見を基に実施するものも多く，企業に関係なく利用できるものが多い．一方 ICT システムの運用ルールや顧客との契約からくる運用上の規制，優先度などは個々の企業によって異なり，また新たな契約やビジネス環境の変化で変更されていく．そのため，企業に関する大まかな背景知識を共有するとともに，それらの企業の内部のメンバや企業同士で信頼関係を築いている他企業がインシデント対応を行うのが効率的であり二次インシデントの発生防止にもつながる．それらを基に以下の 4 つの作業に分類できる．

表 3　CSIRT 活動項目の作業の分類

作業の分類	作業の内容
各社の固有の知見に基づく作業 図 8：左上	活動項目を実施する際，各社の ICT 環境や個別のシステムやその運用状況，業務内容に関係する，各社の状況に合わせて実施する作業
各社共通の知見に基づく作業 図 8：右上	活動項目を実施する際，ICT 関連やマルウェアや APT など世界におけるセキュリティ動向や，企業グループ共通の事項など，各社共通の知見を利用し実施する作業
各社向け作業 図 8：左下	活動項目を実施する際，分析や調整などのように各社ごとのために発生する実施する作業
共通作業 図 8：右下	活動項目を実施する際，イベント検知や情報発信のように，システムで自動化できる作業

表 3 は，上 2 つの作業分類と下 2 つの作業分類に大きく分かれる．上 2 つの作業分類は各企業に関する知見を基に行う作業か，各社共通の知見に基づき実施する作業かの分類であり，作業を行うために必要な知見により分類している．下 2 つの作業は活動項目を実施する際，各社の利用に合わせて行う作業と，各社に関係なく活動項目を実施するために実施する作業に分けている．

4.2 因果ループ図を用いた CSIRT 活動項目の分析

本研究では，前節で述べた各社の状況に応じて CSIRT の活動項目の割当が変化する様子を表現するため，システムダイナミクスの因果ループ図を用いる．

湊宜明の“実践システム・シンキング”［9］では，システムとは“複数の構成要素が相互作用しながら全体としてまとまった機能を果たすもの”とし，システムダイナミクスとは“対象となるシステムを変数という構成要素に分解し変数間の因果関係を連立微分方程式により定義し，コンピュータを用いたシミュレーションによりその動的な振る舞いを時系列で観察する技術”としている．システムダイナミクスのツールである因果ループ図とは，“システムの構成要素を変数として抽出し，変数と変数とを矢印で接続し，その関係性をプラス（＋）かマイナス（－）かの因果関係で表現”するものとしている．

表 3 の CSIRT 活動項目の作業の分類に基づき，集約割当の活動項目を実施する企業がその活動項目を他企業が利用する場合，利用する企業の増減に振る舞いを示す因果ループ図を作成した．

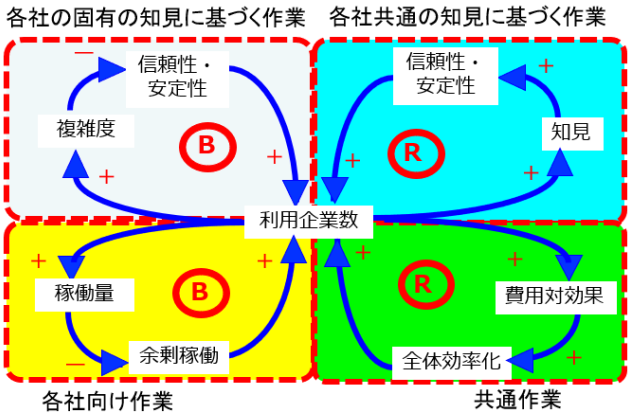

図 8：CSIRT 活動項目の因果ループ図

図 8 の因果ループ図は 2 つのバランス型ループ（○の中に“B”（Balance）の記号があるループ）と，2 つの自己強化型ループ（○の中に“R”（Reinforcing）の記号があるループ）からなる．一般にバランス型ループは各々の要素の関係で，ある程度の規模まで達成するとそれ以上はある要素が増加することを抑える方向に他の要素が影響するループであり，自己強化型ループは各々の要素が互いに増加しあう方向に作用しあうループである．

図 8 の左上のループは利用する企業に対し，実施する各社ごとの知見に基づいた作業に関するループである．個々の利用する企業のカスタマイズ作業が多い活動項目としては，表 2 の“6.4:緩和と回復”，“6.5:情報セキュリティインシデントの調整”，“6.6:危機管理支援”などがある．これらは利用する企業の業務やシステム運用，セキュリティポ

リシー，発災部署などの状況に応じて各社ごとのルールやシステム環境，顧客との調整状況などの知見に基づき実施する必要がある．この活動項目を集約割当として実施する場合，利用する企業数が増えると，それに連動して個々の利用する企業ごとに把握すべき状況やルール，ICT 環境の知見が増加し，複雑度が増加するその結果，この活動項目の作業の安定性や信頼性が低下しインシデントの被害が増加する危険が生じるそのため，集約割当を行う会社を増やし，利用割当企業を分散させるか，個別割当に変更する必要が生じる．

右上のループは利用する企業に関わらず共通の知見に基づき行う作業に関するループである．各社の共通知見を活用する作業が多い活動項目としては，表 2 の“5.1：監視と検知”，“6.3:アーティファクトとフォレンジック痕跡の分析”，“8.1:データ取得”などがある．これらは ICT 技術や社会全体の知見を用いて行う作業である．これは，広く使われる機器やソフトウェア，社会全体の動向に関する作業である．この活動項目を集約作業として実施する場合，利用する企業数が増えても活用する知見は同じであるため，知見がさらに向上するとともに経験が蓄積され，信頼性や安定性が向上する．その結果，この活動項目を集約割当されている企業の評価が高まり，個別割当の企業を利用割当に変更し，その企業を利用し，さらなる集約が行われる．

左下のループは，利用する企業に対し，活動を実施する都度に発生する作業に関するループである．個々の利用する企業のために実施する作業が多い活動項目としては，表 2 の“5.2:イベント分析”，“6.2:情報セキュリティインシデントの分析”，“8.2:分析と統合”などがある．これらは発生したイベントやインシデント，外部動向情報を各社の業務やシステム運用の状況を基に分析を行うため，それらの発生にあわせて作業を行う活動項目である．この活動項目を集約作業として実施する場合，利用する企業数が増えると，それに連動して活動が発生する度に要員が作業を行うため，稼働が増える．その結果，この活動項目を集約割当されている企業の余剰稼働が減り，余剰稼働がなくなると利用する企業数を減らす必要が生じる．その結果，利用割当の企業がある程度に達した後，集約割当する企業を増やし，利用割当の企業を分散させるなどの検討を行う必要が生じる．

右下のループは利用する企業に対し活動を実施する際，個々の利用する企業のためではなく，共通に発生する作業に関するループである．表 2 の“7.1:脆弱性の発見・調査”，“8.1:データ取得”などがある．一般公開されている情報を収集するなど，複数の利用する企業に対し共通して実施する活動項目の作業である．作業自体が共通のため，利用する企業が増えても作業の増加は発生しない．この活動項目を集約作業として実施する場合，利用する企業数が増えるほど費用対効果が良くなる．その結果，この活動項目の集約割当されている企業にさらに利用割当を増やすことでさらに全体効率化が可能となる．

4.3 CSIRT 活動項目の指向性の分析

図 8 の因果ループ図は上半分が活動項目の作業のために必要な知見やスキルに関するものであり，下半分が各活動項目の作業が個々の利用する企業への提供のための作業か複数の利用する企業に共通する作業かに関するものである．各活動項目は一般的には図 8 の因果ループ図の上の左右どちらかのループと下の左右どちらかのループだけになることはなく，４つのループに関係する作業を併せ持っている．各活動項目において，図 8 の４つのループに関する作業のうち，どのループに関連する作業が，その活動項目の作業全体に占める割合が多いかにより，その活動項目の集約割当または個別割当の指向性（集約割当が向くか，個別割当が向くか）を分析することができる．

表 4　活動項目の割当に関する指向性

活動内容	提供時作業	割当の指向性	
利用する企業固有の知見に基づく作業	個々の利用する企業向け作業	A	個別割当，小規模の集約となる集約割当（割当企業の担当者の能力や稼働量に準じる）
	各社共通作業	B	
各社共通の知見に基づく作業	個々の利用する企業向け作業	C	一定規模の集約割当（割当企業の稼働量や担当者の能力に準じる）
	各社共通作業	D	大規模な集約割当

表 4 は活動項目の割当に関する指向性を示している．

- 指向性 A の活動項目
  作業内容も提供する際の作業も個々の利用する企業ごとに併せて行う作業が多いため，基本的には個別割当か少数の企業を対象とした集約割当になる．なお，集約の規模は割当企業の担当者の能力や稼働量に準じる
- 指向性 B の活動項目
  個々の利用する企業の固有の知見に基づく作業で各社共通の作業は存在しない
- 指向性 C の活動項目
  必要なスキルは共通であるが，提供する際に各社向けの作業が発生するため，一定規模までの集約割当になる．なお，集約の規模は割当企業の担当者の能力や稼働量に準じる
- 指向性 D の活動項目
  必要なスキルは共通であり作業も共通のため，集約割当の企業の要員数に制約されることなく集約規模を拡大できる．なお，集約の規模は割当企業の担当者の能力や稼働量に準じる

企業グループの状況や各社が保有すべき活動項目をどのように選定するかによるが，指向性 C，D の活動項目がある場合，有スキル者やリソース確保が可能な企業に集約割当することで，リソースの確保が難しい中小規模の企業が負担を軽くしつつ企業グループで決められたインシデント対応基準を満たすことが可能となる．また，指向性Dの活動項目を割り当てられた企業が企業グループに複数存在する場合，更なる集約を行うことで全体の効率化が図れる可能性が高い．

5. まとめ

本稿では，企業グループを対象として，リソースや要員を確保できない企業のインシデント対応を高める方法として，CSIRT を活動項目に分解し，他企業の活動項目を共有して利用することで，企業グループ全体のインシデント対応能力を向上させる方法を整理した．

２章では昨今のマルウェアや ＡＰＴの傾向から中小規模の企業のインシデント対応能力の確保と改善の重要性を述べ，その課題を解決する方法や事例，先行研究を説明した．CSIRT の現状把握や改善を行う方法として CSIRT を複数の活動項目に分解し，活動項目ごとに分析，改善する方法を複数組織に拡張し，中小規模の企業を含む企業グループ全体でインシデント対応力の目標を達成し，改善する方法について説明した．

３章では本稿で提案する CSIRT 活動項目割当方式について説明した．CSIRT を活動項目に分解し，企業グループの各企業への割当や共通に利用することについての概念や方法を説明した．

４章では提案した CSIRT 活動項目割当方式について分析した．集約割当の活動項目を実施する際，①各社の知見が必要な作業と各社共通の知見に基づく作業の比率，②実施する作業が各社への個別作業か各社共通の作業かを軸とした指向性を提案し個別割当，集約割当の指向性を示した．

提案した CSIRT 活動項目割当方式は，企業グループ全体におけるインシデント対応力について，活動を俯瞰的に状況把握，改善するものである．インシデント対応活動の割当を改善し，インシデント対応の信頼性・安定性の向上や活動の集約を進めることでコストの適正化を進める．

今後は因果ループ図を基にシステムダイナミクスのストックフロー図を作成し，指向性 A，C，D の活動項目がどのような条件で増加が止まるかなど活動項目の分析を深める予定である．また，企業グループに属さない中小規模の企業のインシデント対応力確保など対象を広げる方法について検討する．

参考文献

[1] 一般社団法人 日本損害保険協会 ”国内企業のサイバーリスク意識・対策実態調査 2020“ https://www.sonpo.or.jp/cyber-hoken/data/2020-01/pdf/cyber_report2020.pdf

[2] FIRST，Computer Security Incident Response Team (CSIRT) Services Framework V2.1
日本語版
https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_ja.pdf
英語版
https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

[3] 萩原健太，杉浦芳樹 “CSIRT の最低条件”コンピュータセキュリティシンポジウム 2017

[4] Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek “コンピュータセキュリティ インシデント対応チーム （CSIRT）のための ハンドブック”, CMU/SEI-2003-HB-002
https://www.jpcert.or.jp/research/2007/CSIRT_Handbook.pdf
原文
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6305

[5] Don Stikvoort, “SIM3: Security Incident Management Maturity Model”
http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf

[6] ISOG-J “セキュリティ組織の教科書”
ハンドブック V1.0
https://isog-j.org/output/2017/Textbook_soc-csirt_handbook_v1.0.pdf
ハンドブック別紙 v1.0

[7] 日本シーサーと協議会“CSIRT 人材の定義と確保 v1.5”
https://www.nca.gr.jp/activity/imgs/recruit-hr20170313.pdf

[8] 青山茂義，三河賢治 “大学 CSIRT 体制に対する考察と新潟大学への部局 CSIRT の適用”，学術情報処理研究，2020 年 24 巻 1 号 p. 116-125

[9] 湊宣明 “実践システム・シンキング”講談社，2016

[10] 日本シーサート協議会 “CSIRT 構築から運用まで” NTT 出版，2016

[11] 日本シーサート協議会“CSIRT スターターキット” https://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

[12] Johannes Wiik, Jose J. Gonzalez, Pål I. Davidson, Klaus Peter Kossakowski, “Chronic workload problems in CSIRTs”, Twenty Seventh International Conference of the System Dynamics Society July, at Albuquerque, NM, USA.

[13] 菊池正人, 大久保隆夫, “セキュリティ対策導入にかかる時間と サイバーリスクレベル変動の関係から探る， 過剰なセキュリティ対策の問題とその対策”, 情報処理学会論文誌 Vol.60, No.12, pp.2184.2195 (Dec. 2019)

[14] Klaus Peter Kossakowski, “Organizational Models for Computer Security Incident Response Teams (CSIRTs)”, CMU/SEI-2003-HB-001
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=6295